UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISON

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES ON billing@titanium-brazing.com info@titanium-brazing.com Ishapiro@titanium-brazing.com miditest@titanium-brazing.com sales@titanium-brazing.com

MISC. NO. 2:16-mj-509

Filed Under Seal

APPLICATION

The United States of America, moving by and through, Assistant United States Attorney Douglas W. Squires, respectfully submits under seal this *ex parte* application for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the email accounts described in Attachment A. In support of this application, the United States asserts:

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.

2. Such an application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation.

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by Special Agent Chris Potts, Federal Bureau of Investigation.

6. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

ADDITIONAL INFORMATION

7. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

8. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

9. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique number called an Internet Protocol, or "IP" address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. An IP address is analogous to a telephone number and can be recorded by pen-trap devices, and it indicates the online identity of the communicating device without revealing the communication's content.

11. A network is two or more computers or other devices connected to each other that can exchange information with each other via some transmission method, such as by wires, cables, or radio waves. The equipment that connects a computer or other device to the network is commonly referred to as a network adapter. Most network adapters have a Media Access Control ("MAC") address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. An adapter's unique MAC address allows for proper routing of communications on a local area network and may be used for other purposes, such as authentication of customers by some network service providers. Unlike a device's IP address that often changes each time a device connects to the Internet, a MAC address is fixed at the time of manufacture of the adapter. Because the address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

12. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size.

13. In addition, different Internet applications are associated with different "port numbers," or numeric identifiers. The port number is transmitted along with any communication using that application. For example, port 80 typically is associated with communications involving the World Wide Web.

14. An email message has its own routing header, in addition to the source and destination information associated with all Internet data. The message header of an email contains the message's source and destination(s), expressed as email addresses in "From," "To," "CC" (carbon copy), or "BCC" (blind carbon copy) fields. Multiple destination addresses may be specified in the "To," "CC," and "BCC" fields. The email addresses in an email's message header are like the telephone numbers of both incoming and outgoing calls, because they indicate both origin and destination(s). They can be recorded by pen-trap devices and can be used to identify parties to a communication without revealing the communication's contents.

THE RELEVANT FACTS

15. The United States government, including the Federal Bureau of Investigation, is investigating the illegal export of U.S. goods to an embargoed country, namely Iran. The investigation concerns possible violations by Alexander Shapiro of the International Emergency

Economic Powers Act ("IEEPA"), 50 U.S.C. § 1701-1706, and the Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R, §§ 560.203 and 560.204 and, conspiracy in violation of 18 U.S.C. § 371. Alexander Shapiro is the registered owner of Titanium Brazing Inc. of Columbus, Ohio, within the Southern District of Ohio.

16. The investigation relates to the illegal export of U.S. goods to Iran, an embargoed country per the ITSR. This activity is being conducted using electronics devices and through the sending and receiving of email as provide by internet service providers (ISPs). Investigators believe that matters relevant to the offenses under investigation have been and continue to be discussed using email addresses described in Attachment A, email addresses which are hosted by Hosting Services Inc. Hosting Services Inc. is an internet domain and email hosting provider doing business at 517 West 100 North, Suite 225, Providence, Utah 84332. Investigators believe that the listed subscriber for these email addresses is Alexander Shapiro, a target of the investigation. For example, in 2013 Shapiro received an email from Iran which indicated that Shapiro was involved in illegal trade and a network of businesses supplying U.S. goods to Iran. This activity is likely to be ongoing because from 2013 to the present day Shapiro is still involved in the business of distributing high-end titanium products and materials used in industrial and medical applications.

17. The conduct being investigated involves use of the email accounts described in Attachment A. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from those email accounts.

18. The pen-trap devices sought by this application will record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each

communication to or from the email accounts described in Attachment A, including the date, time, and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account
- Headers of email messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines
- the number and size of any attachments

GOVERNMENT REQUESTS

19. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the email accounts described in Attachment A, to include the date, time, and duration of the communication, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

20. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days from the date of the Court's Order, pursuant to 18 U.S.C. § 3123(c)(1).

21. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order Hosting Services Inc and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen-trap devices, including installation and operation

of the pen-trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by the Federal Bureau of Investigation, pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

22. The United States further requests that the Court order Hosting Services Inc and any other person or entity whose assistance may facilitate execution of this Order to notify the applicant and Special Agent Chris Potts, Federal Bureau of Investigation of any changes relating to the email accounts described in Attachment A, and to provide prior notice to the applicant and Special Agent Chris Potts, Federal Bureau of Investigation before terminating or changing service to the email accounts.

23. The United States further requests that the Court order that the Federal Bureau of Investigation and Special Agent Chris Potts have access to the information collected by the pen-trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

24. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order Hosting Services Inc and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, the resulting pen-trap devices, or this investigation, unless and until authorized by this Court, except that Hosting Services Inc may disclose this Order to an attorney for Hosting Services Inc for the purpose of receiving legal advice.

25. The United States further requests that this application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

26. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this application and Order, and provide copies of this Order to Special Agent Chris Potts, Federal Bureau of Investigation and Hosting Services Inc upon request.

27. The foregoing is based on information provided to me in my official capacity by agents of the Federal Bureau of Investigation.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 26, 2016.

DOUGLAS W. SQUIRES (0073524)
Assistant United States Attorney
Southern District of Ohio

ATTACHMENT A

Hosting Services Inc
Attn: Compliance
517 West 100 North
Suite 225
Providence, Utah 84332

Facility	**Number or identifier**	**Owner, if known**	**Subject of investigation, if known**
email accounts	billing@titanium-brazing.com info@titanium-brazing.com lshapiro@titanium-brazing.com miditest@titanium-brazing.com sales@titanium-brazing.com	Alexander Shapiro	Alexander Shapiro